JD:MEF
F.# 2018R00823

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF: (1) ONE GRAY APPLE MACBOOK PRO LAPTOP, SERIAL NUMBER CPWJLK7KDTY3; (2) ONE GRAY APPLE MACBOOK AIR LAPTOP, SERIAL NUMBER C02N900XG6D5; (3) ONE GRAY APPLE IPAD, SERIAL NUMBER DLXH7Z6MDJ8T; (4) ONE BLACK APPLE IPHONE X; (5) ONE APPLE IPHONE 6, MODEL NUMBER A1549, IMEI NUMBER 354411063842612; (6) ONE APPLE MAC MINI, MODEL A1283, SERIAL NUMBER YM0081P39G5; (7) ONE GRAY APPLE IMAC, MODEL NUMBER A1225, SERIAL NUMBER QP9300WQ0TM; (8) ONE BLACK AND GRAY ULTRA EXTERNAL HARD DRIVE; (9) ONE BLACK WESTERN DIGITAL (WD) EXTERNAL HARD DRIVE, SERIAL NUMBER WCAWZ0891570; (10) ONE BLACK WESTERN DIGITAL EXTERNAL HARD DRIVE, SERIAL NUMBER WCAVY2086429; (11) ONE BLACK WESTERN DIGITAL EXTERNAL HARD DRIVE, SERIAL NUMBER W0A8J1962444; (12) ONE SABRENT EXTERNAL HARD DRIVE, SERIAL NUMBER 60375028908214; (13) ONE SEAGATE EXTERNAL HARD DRIVE, SERIAL NUMBER NA8JECKX; (14) ONE BLACK SEAGATE 160 GB EXTERNAL HARD DRIVE, SERIAL NUMBER 5JS3S1E0; AND (15) ONE BLACK SEAGATE 250 GB EXTERNAL HARD DRIVE, SERIAL NUMBER 5NF0T2HT.

TO BE FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES

Case No.

18M398

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, MATTHEW DERAGON, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—computers, phones, tablets, and external hard drives—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed as a Special Agent since 2014, and I am currently assigned to the Criminal Division of New York. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I am now assigned to the FBI's Violent Crimes against Children Squad (the "Squad"), which investigates individuals suspected of being involved in the online sexual exploitation of children. As part of my duties as a member of the Squad, I investigate violations relating to child exploitation and child pornography, including violations pertaining to the production, possession, distribution, and receipt of child pornography as well as the transportation of minors and interstate travel to engage in illicit sexual conduct, in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2423. I have

received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256[1]) in all forms of media, including computer media. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The statements in this affidavit are based on information provided to me by officers from the New York City Police Department (hereinafter the "NYPD"), and on my own investigation of this matter. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is: (1) ONE GRAY APPLE MACBOOK PRO LAPTOP, SERIAL NUMBER CPWJLK7KDTY3; (2) ONE GRAY APPLE MACBOOK AIR LAPTOP, SERIAL NUMBER C02N900XG6D5; (3) ONE GRAY APPLE IPAD, SERIAL NUMBER DLXH7Z6MDJ8T; (4) ONE BLACK APPLE IPHONE X; (5) ONE

---

[1] "'[C]hild pornography' means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."

APPLE IPHONE 6, MODEL NUMBER A1549, IMEI NUMBER 354411063842612; (6) ONE APPLE MAC MINI, MODEL A1283, SERIAL NUMBER YM0081P39G5; (7) ONE GRAY APPLE IMAC, MODEL NUMBER A1225, SERIAL NUMBER QP9300WQ0TM; (8) ONE BLACK AND GRAY ULTRA EXTERNAL HARD DRIVE; (9) ONE BLACK WESTERN DIGITAL (WD) EXTERNAL HARD DRIVE, SERIAL NUMBER WCAWZ0891570; (10) ONE BLACK WESTERN DIGITAL EXTERNAL HARD DRIVE, SERIAL NUMBER WCAVY2086429; (11) ONE BLACK WESTERN DIGITAL EXTERNAL HARD DRIVE, SERIAL NUMBER W0A8J1962444; (12) ONE SABRENT EXTERNAL HARD DRIVE, SERIAL NUMBER 60375028908214; (13) ONE SEAGATE EXTERNAL HARD DRIVE, SERIAL NUMBER NA8JECKX; (14) ONE BLACK SEAGATE 160 GB EXTERNAL HARD DRIVE, SERIAL NUMBER 5JS3S1E0; AND (15) ONE BLACK SEAGATE 250 GB EXTERNAL HARD DRIVE, SERIAL NUMBER 5NF0T2HT, hereinafter the "Devices." The Devices are currently in FBI custody in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

DEFINITIONS

6. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct" and "visual depiction," are defined as set forth in Title 18, United States Code, Section 2256.

7. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ."[2]

PROBABLE CAUSE

8. On or about November 14, 2017, the NYPD received a "Priority Level 1" notification report (highest urgency) from the National Center for Missing and Exploited Children ("NCMEC") Cyber Tipline, identified as Tip No. 25544679, informing the NYPD that Facebook Inc. had identified a 33-year old adult male named Jonathan Deutsch (hereinafter "Deutsch") who was enticing multiple children to send and produce, via social

---

[2] See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

media accounts, pornographic content. Facebook reported that Deutsch was likely a math teacher, teaching at Gramercy Arts High School in New York, NY, and utilized the email address JDeutsch@schools.nyc.gov. Facebook described the person being reported as follows:

> User or Person Being Reported
> Name: Jonathan Deutsch
> Address: New York, NY US
> Phone: 347-439-5824
> Email Address: deutsch.jonathan@gmail.com
> Screen/User Name: jdeutsch1
> ESP User ID: 47101549
> Profile URL: https://www.facebook.com/jdeutsch1
> IP Address: 69.124.40.137

9. As part of the same report, Facebook reported that "JDeutsch (UID 47101549)" (hereinafter "Facebook Account 1") was linked by machine cookies to the following accounts: "Sam Morgan (UID 1000019241760508)" (hereinafter "Facebook Account 2"); "Sam Morgan (UID 100016938766073)," registered as a male with a date of birth of June 11, 2002 (15 years old) (hereinafter "Facebook Account 3"); and "Jay Stern (UID100006276969178)" (hereinafter "Facebook Account 4"), registered as a male with a date of birth of March 3, 1983 (33 years old). Facebook further reported that Facebook Account 1 and Facebook Account 2 were linked by the same IP address, to wit: 24.44.166.55 (New York, New York); Facebook Account 3 and Facebook Account 4 were linked by the same IP address, to wit: 47.18.138.69 (New York, New York); and Facebook Account 2 and

Facebook Account 3 were linked by the same IP address, to wit: 69.112.4.72 (Brooklyn, New York).

10. Facebook also reported that Facebook Account 4 was used to entice accounts associated with at least six child victims ranging in age from 15 to 17 years old[3], to produce and send Child Exploitation Images (CEI) via private messages. Those reports are summarized in the chart below:

NCMEC Report No.	Incident Date	Sender's Name and Approximate Age	Number of Images	Recipient IP Address
25162055	6/16/2016	[redacted](17)	6	47.18.138.69
25162148	10/24/2016	[redacted](16)	2	47.18.138.69
25162000	1/26/2017	[redacted](15)	6	47.18.138.69
25161956	1/27/2017	[redacted](16)	3	47.18.138.69
25161923	9/12/2016	[redacted](17)	3	47.18.138.69
25161839	1/6/2017	[redacted](17)	9	47.18.138.69

11. In additional reports to the NCMEC Cyber Tipline, Facebook reported that Facebook Account 3, also known as "Sam Morgan," was in touch with at least two apparent minors, both of whom sent Deutsch CEI. Those reports are summarized in the chart below:

[3] Note that the ages associated with the referenced accounts are based on information provided by the user who registered the relevant account.

NCMEC Report No.	Incident Date	Sender's Name and Approximate Age	Number of Images	Recipient IP Address
22044583	5/24/2017	[redacted] (15)	5	47.18.138.69
22044596	5/24/2017	[redacted] (14)	3	47.18.138.69

12. In additional reports to the NCMEC Cyber Tipline, Facebook reported that a Facebook account for "James Benjamin (UID 100015668078667)" (hereinafter "Facebook Account 5"), was in contact with at least four apparent minors, all of whom sent CEI to Facebook Account 5. According to those same reports, Facebook Account 5 is associated with the same IP address as Facebook Account 3 and Facebook Account 4. Those reports are summarized in the chart below:

NCMEC Report No.	Incident Date	Sender's Name and Approximate Age	Number of Images	Recipient IP Address
22044490	4/10/2017	[redacted] (14)	5	47.18.138.69
22044666	4/17/2017	[redacted] (16)	1	47.18.138.69
22044689	5/4/2017	[redacted] (16)	2	47.18.138.69
25161656	4/12/2017	[redacted] (15)	5	47.18.138.69

13. On or about November 28, 2017, the Honorable Jonathan Hecht of the Supreme Court of the State of New York authorized a search warrant that allowed police officers of the NYPD to search the records of Facebook Inc. for property associated with

Facebook Account 1, Facebook Account 3, Facebook Account 4, and Facebook Account 5 (hereinafter "Facebook Search Warrant"). (See attached "Exhibit 1")

14. According to information received pursuant to the Facebook Search Warrant, in conversations on or about January 26, 2017, between Facebook Account 4 and [redacted] the minor identified herself as 16 years old, and Deutsch responded that she is not too young. Deutsch continued by describing himself as a 33-year old middle school math teacher, and stated, in sum and substance, "daddy got an interesting offer that he turned down today, in which a student told him that her younger sisters wanted to learn about sex." [redacted] replied, in sum and substance, "I'm the only girl daddy likes and if they try to take you I will tear them apart." Deutsch responded, in sum and substance, "but they were little…it was so exciting." [redacted] then asked, "Daddy do you have snapchat, stay right here I have a surprise." The minor then sent a number of nude photographs of herself and fully nude videos of herself masturbating in various different positions.

15. According to information received pursuant to the Facebook Search Warrant, in conversations on or about January 24, 2017, between Facebook Account 4 and [redacted] who claimed to be 14, Deutsch told the minor that he wanted a "full body mirror selfie." [redacted] then sent a full-frontal nude image with her face showing, which appears to have been taken using a mirror, and the face in which is the same as prior images shared by [redacted]

16. According to information received pursuant to the Facebook Search Warrant, in conversations on or about January 24, 2017, between Facebook Account 4 and [redacted] who identified herself as 14, the minor sent an image of female genitalia where two

fingers are used to spread the female's genitalia so the clitoris is visible. Deutsch responded that he "didn't just mean pics," and the minor said she "cant do vids ether." I am informed by NYPD that they successfully contacted the individual associated with the Facebook account [redacted] User ID 100009670818441, whose legal name is [redacted] and date of birth is February 24, 2002, through local Florida law enforcement. During an interview conducted on December 29, 2017, [redacted] informed local law enforcement that Deutsch claimed to be a 33-year-old math teacher, asked [redacted] to send him sexy pictures of herself, including those of her vaginal area, and [redacted] did send Deutsch pictures of herself.

17. According to information received from Facebook, Facebook Account 3 was linked to two email addresses ("Sammorgan052@gmail.com" and "TheSammorgan2002@gmail.com"), both of which were linked to the following IP addresses: 69.112.4.72 and 24.44.166.55. Additionally, the email address "Deutsch.Jonathan@gmail.com" is linked to those same two IP addresses. Finally, information from Facebook confirmed that "Deutsch.Jonathan@gmail.com" is the email address associated with Facebook Account 1, Deutsch's Facebook account.

18. On or about November 29, 2017, representatives from Google confirmed that the email address "Deutsch.Jonathan@gmail.com" is associated with the same phone number given by Deutsch when registering Facebook Account 1 (347-439-5824) as well as Deutsch's work email address ("jdeutsch@schools.nyc.gov"). Further, the IP addresses most often used to access the account associated with "Deutsch.Jonathan@gmail.com" are 69.112.4.72 and 24.44.166.55.

19. On or about November 29, 2017, representatives from Google confirmed that one of the email addresses associated with Facebook Account 3, "Sammorgan052@gmail.com," is accessed by the following IP address: 69.112.4.72. At the same time, Google representatives confirmed that a second email address associated with Facebook Account 3, "TheSammorgan2002@gmail.com," is accessed by the following IP addresses: the IP address of 69.112.4.72, 24.44.166.55 and 47.18.138.69.

20. I am informed by Optimum, pursuant to a subpoena, that the aforementioned IP addresses (24.44.166.55, 69.112.4.72, and 47.18.138.69) are associated with the Optimum Wireless Service subscriber Jonathan Deutsch, at 2785W 5th Street, Apartment 12C, Brooklyn, New York. Further, in establishing that account, Deutsch provided the same phone as that associated with his Google and Facebook account, *i.e.*, 347-439-5824.

21. Additionally, according to the New York Department of Motor Vehicles, Deutsch's address is 2785W 5th Street, Apartment 12C, Brooklyn, New York.

22. On or about December 22, 2017, the Honorable Danny Chun of the Supreme Court of the State of New York authorized a search warrant that allowed police to search the premises of 2785W 5th Street, Apartment 12C, Brooklyn, New York, for, *inter alia*, any and all computers and storage devices, capable of storing data, writings and images; any and all cellular telephones, cameras, video recorders, or electronic devices capable of storing data, information, and images; and any and all video or photograph storage devices, video or photography equipment. (See attached "Exhibit 2")

23. NYPD executed the December 22, 2017 warrant on or about December 29, 2017, at which point they recovered the Devices from Deutsch's home, 2785W 5th Street,

Apartment 12C, Brooklyn, New York. At or about the same time, NYPD arrested Deutsch. After being read Miranda warnings, Deutsch confirmed that he is the only person that lives at 2785W 5th Street, Apartment 12C, Brooklyn, New York, that his date of birth is December 19, 1983, and that he is a New York City school teacher.

24. In light of the above, there is probable cause to believe that the Devices were used to access Facebook Accounts 1-5, and thereby solicit child pornographic images from minors.

25. Given the ease with which collectors of child pornography typically transfer their materials between and among electronic devices, which they may do through the use of external hard drives, there is probable cause to believe that all of the Devices contain child pornographic images.

26. The Devices are currently in the lawful possession of the FBI. They came into the FBI's possession through the NYPD, which obtained them from Deutsch's residence on December 29, 2017.

27. The Devices are currently in the Eastern District of New York. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the NYPD.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard

drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that

are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise.

Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

29. Based on my training, experience, and research, I know that Devices 1, 2, 3, and 6, have capabilities that allow them to serve as a digital camera, portable media player, and PDA. Based on my training, experience, and research, I know that Devices 4 and 5, have capabilities that allow them to serve a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

30. Based on my training, experience, and research, I know that Devices 8-15 are capable of storing images and multimedia files, which can then be viewed by connecting them to a variety of electronic devices, including but not limited to personal computers.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when

a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been

viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

36. Based on my training and experience and conversations that I have had with other federal agents and law enforcement offices, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

37. I have learned that collectors of child pornography typically retain their materials and related information for many years.

38. I have learned that collectors of child pornography typically transfer their materials between and among electronic devices with ease, which they may do through the use of external hard drives.

39. I also have learned that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names or individuals with whom they have been in contact and who share the same interests in child pornography.

40. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

41. Further, based on my training, knowledge, expertise and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

CONCLUSION

42. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

43. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into child pornography. Based upon my

training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

MATTHEW DERAGON
Special Agent
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to before me on May 2, 2018:

UNITED STATES MAGISTRATE JUDGE

EXHIBIT 1

KSC 1030

SUPREME COURT OF THE STATE OF NEW YORK
PART MISC, COUNTY OF KINGS

SCORED IN P. Daly

STATE OF NEW YORK)
) - ss.:
COUNTY OF KINGS)

20 17

Detective Sheldon Spence, Shield Number 4739, of the Special Investigations Division, being duly sworn, deposes and says:

1. I am a detective employed by the New York Police Department and I have been a police officer for approximately twelve (12) years. I have been assigned to the Special Investigations Division for approximately three (3) years. My current responsibilities include, *inter alia*, the investigation of the promotion of sexual performance by a child through the use of electronic devices and the internet, as well as investigating the possession and distribution of child pornography through the use of electronic devices and the internet. During my service with the Special Investigations Division, I have conducted over sixty (60) investigations into the sexual exploitation of minor children through the use of the internet. I have also been involved in the execution of approximately forty (40) search warrants.

2. My training includes, the following:

a. I have participated in over twenty (20) interviews involving subjects who have discussed the methods by which they engage in the possession, storage and distribution of child pornography.

b. I have received specialized training in the area of "on-line" criminal investigations, including the investigation of internet sexual predators, and the production, possession, and distribution of still and video images depicting underage children engaged in sexual activity or sexual conduct, and/or the lewd depiction of the genitals of these underage children, especially when these illicit images are transmitted or received over the internet. I have received training in the area of computer evidence and handling computer forensics, including the ability to conduct forensically sound "field previews" of computers suspected of being involved in the aforementioned types of criminal activity.

3. This affidavit is made in support of an application for a search warrant to authorize police officers of the New York City Police Department to search the records of Facebook Inc., for the property described below in Paragraph 5.

4. I state that based on my training and experience, there is reasonable cause to believe that property constituting evidence of an offense, unlawfully possessed, that has been used or is possessed for the purpose of being used to commit or conceal of the commission of an offense against the laws of this State or another State, and/or evidence that tends to demonstrate that an offense was committed or a particular person participated in the commission of an offense, specifically, Promoting a Sexual Performance by a Child (P.L. § 263.15), Possessing a Sexual Performance by a Child (P.L. § 263.16) and related charges, which occurred in Kings County, New York, will be found within and upon the records of Facebook, Inc. related to the accounts associated with the following URLs:

http://www.facebook.com/people/James-Benjamin/100015668078667 ("subject Facebook Account 1"),

http://www.facebook.com/profile.php?id=100016938766073 ("subject Facebook Account 2"),

https://www.facebook.com/jdeutsch1?lst=36402882%3A47101549%3A1511196868 ("subject Facebook Account 3"), and

http://www.facebook.com/jay.stern.315 ("subject Facebook Account 4"), collectively, "subject Facebook accounts"

Prepared by ADA Grace K. Hogan
November 28, 2017
LEAU SW Nos. 440-441-442-443/2017

including but not limited to user identity, name, postal code, country, user id, e-mail address, date of account creation, login records including IP addresses, the hardware and software used to access Facebook, including make, model, operating system, OS version, application information, mac addresses, serial numbers, cookies, telecommunications carrier, MEID, ESN, IMSI, SIM, IMEI, and any other identifiers or device information, logs showing IP Address and date stamps for account accesses, any and all stored electronic and wire communications and information, including email, instant messaging, or other communications, contents of any and all postings, private messages in the user's inbox, private messages in trash mail, and sent mail folders, stored user files, photos or videos uploaded to their profile, including the EXIF metadata, EXIF tags, timestamps, geolocation data, and other users' comments, classified advertisements, historical private message header information, messages posted on Facebook forums or in Facebook groups, private journals or blogs, address book, calendar contents, attachments, vanities and wall posts, user passwords, friend listing with name and Facebook ID number for the period beginning **January 1, 2017 to the present.**

5. Based on my training and experience, I believe the following cyber-property sought and to be seized from within and upon the aforementioned records of Facebook Inc. consists of:

a. documents containing information about the operation and ownership of a personal computer(s);

b. video and/or photographic images common in the production, use and distribution of child pornography;

c. computer-related information including, but not limited to, websites, e-mail addresses, IP addresses and screen names used to obtain or possess child pornography or images and videos relating to or demonstrating a sexual interest in children;

d. identification of computer software systems, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs;

e. records and materials, in any format or media, pertaining to the payment for or possession, receipt, transmission, shipment, or distribution of visual depictions of minors engaged in sexually explicit conduct or relating to or demonstrating a sexual interest in children;

f. records, in any format or media, identifying persons transmitting any visual depiction of minors engaged in sexually explicit conduct or relating to or demonstrating a sexual interest in children;

g. records, in any format or media, evidencing ownership or use of computer equipment, software, or the Internet including, but not limited to, sales transactions, registration records, records of payment for Internet access, records of payment for other online subscription services;

h. any and all data, information, or images evidencing Internet usage history;

i. any and all data, information, or images that evidence ownership and use of the access device, including, but not limited to, calendar entries, e-mail addresses, stored telephone numbers and names, nicknames, and/or labels assigned to said numbers, photographs, videos, bank account documents, bills and invoices, recorded voice memos, text messages, instant messenger messages, letters, and stored voicemails;

j. any and all data, information, or images evidencing passwords that may be used to unlock or decrypt data, information, or images stored on the device, which may or may not be stored in a locked or encrypted fashion, whether said passwords are letters, numbers, characters, words, or data strings (sequence of characters);

k. any and all images, Internet histories, Internet site bookmarks, search requests, temporary Internet files, cookies, newsgroups, postings to newsgroups, folder structures and names, and file names stored on the device relating to child pornography (visual depictions of minors engaged in sexual conduct as defined in Penal Law §263.00[3]) or a sexual interest in children;

l. e-mail containing writing regarding child pornography or a sexual interest in children;

m. evidence of affiliations, memberships, buddy lists, profiles, chat sessions, chat services, billboards, newsgroups, and websites pertaining to child pornography or a sexual interest in children;

n. any and all records and materials, in any format or media (including, but not limited to, e-mail, instant message chat logs, electronic messages, other digital data files, and web cache information), identifying persons transmitting any visual depiction of minors engaged in sexually explicit conduct or demonstrating a sexual interest in children;

o. records of communication between individuals concerning the topic of child pornography, having sex with children, the existence of sites on the Internet that contain child pornography or that cater to people with an interest in child pornography, or membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to their members and constituents;

p. records of correspondence and communication with known and identified underage minor children;

q. evidence of any online storage, e-mail, or other remote computer storage subscription, including, but not limited to, unique software relating to such subscription, storage, or email, user logs, archived data that shows connection to such service, or user login and password for such service;

r. any and all data, information, or images evidencing or revealing the unauthorized use of the device by a person other than an owner or authorized user, through the use of viruses, Trojan horses, or other malicious software or infiltration methods.

6. With respect to the stored electronic data, information, and images contained in said Facebook Inc. records described above, it is also requested that this Court grant permission to retrieve the above-described data, information, and images, and print them or otherwise reproduce them by converting them or copying them into storage in another device.

7. This affidavit is based on my training, experience and personal observations, and information supplied to me from sources mentioned in the paragraphs below.

8. Based on my training and experience, including my interviews with suspects regarding collections of child pornography, I have become very familiar with the methods used by individuals to obtain, store, and trade in child pornography, including the following:

a. People who collect and trade in child pornography typically do not destroy or delete image or video files depicting child sexual abuse.

b. Collectors of child pornography typically retain their materials and related information for many years. These individuals retain their material indefinitely for the purpose of sexual gratification and sharing with others.

c. Individuals in possession of files containing sexual abuse are likely to save and maintain these files on their computer, portable storage devices, or in the cloud so it is accessible to them in their home or office.

d. Because of the illegality and the severe social stigma child pornography images carry, these individuals hide them in secure places, such as hidden files on the hard drive of the computer, external storage media or cloud storage.

e. I have experience and knowledge in the methods of communications that may be utilized through a computer, including but not limited to emails, chat rooms, instant messaging, peer to peer networks, as well as basic skills in the recording and storage of online communications.

f. Files are maintained indefinitely on a computer and/or in the cloud.

g. Deleted files can usually be recovered during a forensic examination.

9. One of the goals of the investigation is to determine whether there are other persons within this jurisdiction possessing or distributing child pornography and ultimately identify any persons who are engaged in the direct exploitation of children by creating and publishing child pornography. Lists of emails addressed, buddy lists, and telephone numbers of persons they have contacted whether as potential victims or persons who share similar interests and materials are frequently maintained on their computers and storage media, as well as on their cell phones, electronic calendar/address books, personal communication service devices, social media accounts, and the cloud.

10. With a computer connected to the internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of ways, including modem, local area network, wireless and numerous other methods.

11. Any computer accessing the Internet is assigned a unique Internet Protocol (IP) address. An IP address is a set of numbers which identify a specific computer on the internet. IP addresses follow the format of a series of sixteen numerals, which are organized in four groups of three numerals that are separated by a period, or: ###.###.###.###, wherein each of the number are between 0 and 255. Computers use IP addresses to identify each other on the internet. Thus, because a computer accessing "Outlook" (Microsoft) must be connected to the Internet, that device is identifiable by its IP address. Thus, investigators are able to determine the IP address of any computer using Microsoft services by issuing a subpoena to Microsoft. Then, investigators can search a public database compiled by the American Registry of Internet Numbers to determine the Internet Service Providers ("ISP") assigned to that specific IP address.

12. When a subscriber of an ISP wishes to access the internet via their service, the ISP will assign that account an IP address which identifies that account holder on the internet. By providing the ISP with the dates, times and IP addresses which a suspect used to access the internet, the ISP will be able to provide the identifying information for the account holder who was assigned that specific IP address at that date and time, if the records still exist on their system.

13. On or about November 15, 2017, I received a "Priority Level 1" notification report (highest urgency) from The National Center for Missing and Exploited Children ("NCMEC") Cyber Tipline, identified as Tip No. 25544679, informing me that Facebook Inc. had identified a 33-year old adult male named "Jonathan Deutsch" ("perpetrator") who was enticing multiple children to send and produce, via social media accounts, pornographic content. Facebook Inc. reported that based on the conversations between this perpetrator and the child victims, and the social media profiles of the perpetrator and the victims, the perpetrator may be a math teacher, possibly teaching at Gramercy Arts High School in New York, NY. Facebook Inc. further reported a connection between the aforementioned pornographic communications with an email address of JDeutsch@schools.nyc.gov in that the perpetrator used this NYC schools email address to register the aforementioned URL https://www.facebook.com/jdeutsch1?lst=36402882%3A47101549%3A1511196868, subject Facebook Account 3, and that this NYC schools email is registered to the domain GramercyArtsHS.org.

14. I am informed by the official records of the New York State Department of Motor Vehicles and the New York State Education Department that the perpetrator, Jonathan Deutsch, resides at 2785 West 5th Street, Apartment 12C, Brooklyn NY.

15. Pursuant to investigation, I learned that the I.P. address linked to these illegal communications is geo-located to Brooklyn NY.

16. I am further informed by NCMEC that the aforementioned address is the domicile of Jonathan Deutsch, and was his current address on the date their report was made, November 15, 2017.

17. I am further informed by Facebook Inc. that the following children, both males and females, were engaged by the perpetrator in pornographic communications, and the identifying information of said minors, and the recent dates and times of those communications; other identifying information has been omitted from this application:

Child Victim
Name: [redacted]
Email Address: [redacted]
Profile URL: [redacted]
11-13-2017 03:30:00 UTC

Child Victim
Name: [redacted]
Email Address: [redacted]
Screen/User Name: [redacted]
Profile URL: [redacted]
11-14-2017 02:25:00 UTC

Child Victim
Name: [redacted]
Email Address: [redacted]
Screen/User Name: [redacted]
Profile URL: [redacted]
02-20-2017 00:28:00 UTC

Child Victim
Name: [redacted]
Email Address: [redacted]
Screen/User Name: [redacted]
Profile URL: [redacted]
11-14-2017 13:37:00 UTC

Child Victim
Name: [redacted]
Screen/User Name: [redacted]
Profile URL: [redacted]
11-11-2017 00:30:00 UTC

Child Victim
Name: [redacted]
Email Address: [redacted]
Screen/User Name: [redacted]

Prepared by ADA Grace K. Hogan
November 28, 2017
LEAU SW Nos. 440-441-442-443/2017

Profile URL: [redacted]
10-19-2014 14:27:00 UTC

Child Victim
Name: [redacted]
Email Address: [redacted]
Screen/User Name: [redacted]
Profile URL: [redacted]
11-14-2017 03:49:00 UTC

Child Victim
Name: [redacted]
Screen/User Name: [redacted]
Profile URL: [redacted]
11-06-2017 23:07:00 UTC

and Facebook Inc. further reported to NCMEC that the adult subject of their investigation is:

User or Person Being Reported
Name: Jonathan Deutsch
Address: New York, NY US
Phone: 347-439-5824
Email Address: deutsch.jonathan@gmail.com
Screen/User Name: jdeutsch1
ESP User ID: 47101549
Profile URL: https://www.facebook.com/jdeutsch1
IP Address: 69.124.40.137

18. I am further informed by Facebook, that the person of "Jonathan Deutsch," the perpetrator, has a total of four (4) Facebook accounts under different names and profiles. I am further informed by Facebook Inc. that Facebook was able to link these profiles to each other, and back to Jonathan Deutsch by analyzing machine cookies and IP addresses from which the illicit communications were sent and received.

19. I am further informed by Facebook that the four Facebook profiles linked to perpetrator Jonathan Deutsch are:

- "James Benjamin" using Subject Facebook Account 1;
- "Sam Morgan" using Subject Facebook Account 2;
- "J. Deutsch" using Subject Facebook Account 3; and
- "Jay Stern" using Subject Facebook Account 4

20. The content of the communications between Jonathan Deutsch, sent from and between the aforementioned aliases of Jonathan Deutsch, includes:

In conversations between "Jay Stern" and [redacted] the minor identified herself as 16 years old, and the perpetrator responded that she is not too young. Jay Stern continues by describing himself as a 33-year old middle school math teacher. Jay Stern further states - daddy got an interesting offer that he turned down today, in which a student told him that her younger sisters wanted to learn about sex. The minor replies - I'm the only girl daddy likes and if they try to take

you I will tear them apart. Jay Stern responds- but they were little...it was so exciting. The minor then asks - Daddy do you have snapchat, stay right here I have a surprise, whereupon the minor sent a number of nude photographs of herself and fully nude videos of the minor masturbating herself in various different positions.

In conversations with one of the aforementioned male minors, the content includes the perpetrator stating -he wants to drain the minor's cock in the perpetrator's mouth. In other conversations, the perpetrator states, in sum and substance, just wear sum thin shown of your tits and strip, I wanna c u looking sexy, that the minor should send the perpetrator a video of the minor masturbating and "squirting," and do something to get the perpetrator nice and hard.

21. I am further informed by Facebook that the majority of these illicit communications occurred between 2016 and 2017, and involved minors between the ages of 15 and 17 years.

22. Based on my training, experience, and gathered intelligence, I have observed the following:

- Facebook accounts contain two types of information, one type, which is accessible to general public, the other type that is protected by a privacy wall and only accessible to individuals who are allowed such access by the account holder;
- Facebook accounts are used by individuals to communicate with one another, post photographs and other personal information, exchange messages, e-mail and disseminate other communications including photographs and videos.
- Facebook pages and other social media are known to be frequently used by individuals involved in child pornography, particularly as a forum to attract and communicate with minors who are typically avid users of social media platforms.

23. Based on the foregoing, my training and experience as a detective, NYPD intelligence, and Facebook inquiries already conducted, the records within and upon the subject Facebook accounts will contain evidence of criminal activity, namely communications related to the above-mentioned possession and transmission of child pornographic images.

24. I believe that the requested records are material and relevant in the above-mentioned investigation in that the records will contain stored communications related to the above-mentioned crimes.

25. Based on the foregoing, there is probable cause to believe that the subject Facebook accounts contain evidence of criminal activity.

I request that any examination by this Court be incorporated into this application. I further request that this application and minutes of any examination conducted by this Court be sealed except for one copy, which will be maintained by the Kings County District Attorney's Office until needed for the prosecution resulting from the execution of this warrant.

I request that the Court orders Facebook, Inc. not to disclose the existence of this Order or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise directly by the Court.

I also request that the Court authorize a search for the internet browsing history, keyword searches, stored documentation, file images, addresses, pages and any other electronic information, photo images (including video images), any information concerning computer passwords, encryption, web-sites, screen names or electronic mail addresses, any deleted files and all images, databases of personal identification information and contact list, any data related to the crimes described herein, and any other data which would indicate ownership or use of the searched Subject Facebook Inc. Accounts concerning the identification of individual(s) involved in said crimes;

I also request that the search continue past the recovery of the first pertinent records and documents in any format, including electronically stored data and/or communications, information, images, text messages, e-mails, instant messages, contacts (names, addresses, telephone numbers, e-mail addresses), and continue until all such pertinent electronically stored evidence is recovered;

I also request that in the event that during the execution of the warrant with regards to the search of the Subject Facebook Accounts, it is necessary to utilize the assistance of others with expertise in decoding and/or obtaining password protections and/or encryptions, and in transferring, downloading, converting, dumping or draining the contents of the Subject Facebook Accounts, such expert assistance may be sought and that such experts may be members of law enforcement organizations, industry trade associations, or from companies which host these telecommunications.

WHEREFORE, I respectfully request that the Court issue a warrant and Order of seizure in the form annexed, authorizing the search of the above-stated property, specifically Facebook, Inc. records for the subject accounts, for the period beginning **January 1, 2017 to present**, and directing that if such property or evidence or any part thereof be found, that it be seized and brought, or an inventory thereof, before the Court, together with such other and further relief that the Court may deem proper.

No prior application in this matter has been made.

Sworn to before me
Brooklyn, New York
November 28, 2017
Time:

[redacted]
Detective Sheldon Spence,
Shield Number 4739,
NYPD Special Investigations Division

[redacted] HON. JOHN T. HECHT
HON. JONATHAN HECHT
Justice, Supreme Court

NOV 28 2017

COURT REPORTER

Prepared by ADA Grace K. Hogan
November 28, 2017
LEAU SW Nos. 440-441-442-443/2017

EXHIBIT 2

SUPREME COURT OF THE STATE OF NEW YORK
PART MISC, COUNTY OF KINGS

KSC 1097
Logged in by: P. Daly
2017

STATE OF NEW YORK)
) - ss.:
COUNTY OF KINGS)

Detective Sheldon Spence, Shield Number 4739, of the Special Investigations Division, being duly sworn, deposes and says:

1. I am a detective employed by the New York Police Department and I have been a police officer for approximately twelve years. I have been assigned to the Special Investigations Division for approximately three years. My current responsibilities include, *inter alia*, the investigation of the promotion of sexual performance by a child through the use of electronic devices and the internet, as well as investigating the possession and distribution of child pornography through the use of electronic devices and the internet. During my service with the Special Investigations Division, I have conducted over sixty investigations into the sexual exploitation of minor children through the use of the internet. I have also been involved in the execution of approximately forty search warrants.

2. My training includes, the following:

a. I have participated in over twenty interviews involving subjects who have discussed the methods by which they engage in the possession, storage and distribution of child pornography.

b. I have received specialized training in the area of "on-line" criminal investigations, including the investigation of internet sexual predators, and the production, possession, and distribution of still and video images depicting underage children engaged in sexual activity or sexual conduct, and/or the lewd depiction of the genitals of these underage children, especially when these elicit images are transmitted or received over the internet. I have received training in the area of computer evidence and handling computer forensics, including the ability to conduct forensically sound "field previews" of computers suspected of being involved in the aforementioned types of criminal activity.

3. This affidavit is made in support of an application for a search warrant to authorize police officers of the New York City Police Department and Special Agents of the U.S. Federal Bureau of Investigation, to search the premises of 2785 W 5TH Street, Apartment 12C, Brooklyn, NY for the property described below in Paragraph 5.

4. I state that based on my training and experience, there is reasonable cause to believe that property constituting evidence of an offense, unlawfully possessed, that has been used or is possessed for the purpose of being used to commit or conceal of the commission of an offense against the laws of this State or another State, and/or evidence that tends to demonstrate that an offense was committed or a particular person participated in the commission of an offense, specifically, Promoting a Sexual Performance by a Child (P.L. § 263.15), Possessing a Sexual Performance by a Child (P.L. § 263.16) and related charges, which occurred in Kings County, New York, will be found inside of **2785 W 5th Street, Apartment 12C, Brooklyn, Kings County, NY** ("subject location").

5. The property sought and to be seized consists of:

a. any and all computers as defined in Penal Law § 156.00(1)[1] or electronic storage devices

[1] Penal Law §156.00(1) states, "Computer" means a device or group of devices which, by manipulation of

capable of storing any of the above-described property, as well as their components and accessories, including, but not limited to, cords, monitors, keyboards, software, programs, disks, zip drives, flash drives, thumb drives, hard drives, and any other device used to store computerized data, writings, and images;

b. any and all cellular telephones, cameras, video recorders, video game consoles, and other electronic devices and/or equipment capable of storing data, information, and images, and their components and accessories, including, but not limited to, wires, cords, monitors, software, hard drives, and chargers;

c. any and all books, manuals, guides, or other documents containing information about the operation and ownership of a computer, cellular telephone, camera, video recorder, video game console, or other electronic storage device present in the subject location, including, but not limited to, computer, cellular telephone, and software user manuals;

d. any and all video or photograph storage devices, video or photography equipment, or other equipment that aids in the production of child pornography, including, but not limited to, VCRs, DVDs, and videotapes, and their components and accessories, including, but not limited to, wires and cords;

e. any and all handwritten or typed notes containing computer-related information including, but not limited to, websites, e-mail addresses, and screen names used to obtain or possess child pornography or images relating to or demonstrating a sexual interest in children;

f. any written material, including, but not limited to, photographs, drawings, magazines, books, or other written materials relating to child pornography or a sexual interest in children;

g. any and all computer software, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs;

h. any computer-related documentation, which consists of written, recorded, or printed material that explains or illustrates how to configure or use computer hardware, software, or other related items;

i. any and all records and materials, in any format or media (including, but not limited to, envelopes, letters, or papers), pertaining to the payment for or possession, receipt, shipment, or distribution of visual depictions of minors engaged in sexually explicit conduct or relating to or demonstrating a sexual interest in children;

j. all originals, copies, and photographic negatives of visual depictions of minors engaged in sexually explicit conduct or relating to or demonstrating a sexual interest in children;

k. any and all records and materials, in any format or media (including, but not limited to, envelopes, letters, or papers) identifying persons transmitting any visual depiction of minors engaged in sexually explicit conduct or relating to or demonstrating a sexual interest in children;

l. any and all records, in any format or media, evidencing ownership or use of computer equipment, software, or the Internet found in the subject location, including, but

---

electronic, magnetic, optical or electrochemical impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data.

not limited to, sales receipts, registration records, records of payment for Internet access, records of payment for access to newsgroups or other online subscription services, and handwritten notes;

m. Evidence of ownership and use of the Subject location, or the use of property located therein by any person, including, but not limited to, keys, telephone bills, utility bills, bank statements, leases, deeds, or rent receipts related to the subject location or other real property, mail addressed to or from the subject location, or other documents bearing the address of the subject location, identification bearing the name or photograph of any person, telephone books, address books, date books, calendars, personal papers, driver's licenses, vehicle registration, vehicle insurance documents, vehicle repair documents, toothbrushes, hairbrushes, videotapes and photographs of persons, fingerprints, handprints, footprints, shoe impressions, hairs and fibers, swabs and/or samples of DNA, and other forensic and trace evidence.

6. With respect to the seizure and search of computers, electronic storage devices, cellular telephones, cameras, video recorders, video game consoles, and other electronic devices and/or equipment capable of storing the above-described property, in addition to searching for the items described above, it is requested that authorization be granted to search these devices for the following:

a. any and all data, information, or images evidencing Internet usage history;

b. any and all data, information, or images that evidence ownership and use of the device, including, but not limited to, calendar entries, e-mail addresses, stored telephone numbers and names, nicknames, and/or labels assigned to said numbers, photographs, videos, bank account documents, bills and invoices, recorded voice memos, text messages, instant messenger messages, letters, and stored voicemails;

c. any and all data, information, or images evidencing passwords that may be used to unlock or decrypt data, information, or images stored on the device, which may or may not be stored in a locked or encrypted fashion, whether said passwords are letters, numbers, characters, words, or data strings (sequence of characters);

d. any and all images, Internet histories, Internet site bookmarks, search requests, temporary Internet files, cookies, newsgroups, postings to newsgroups, folder structures and names, and file names stored on the device relating to child pornography (visual depictions of minors engaged in sexual conduct as defined in Penal Law §263.00[3]) or a sexual interest in children;

e. e-mail containing writing regarding child pornography or a sexual interest in children;

f. evidence of affiliations, memberships, buddy lists, profiles, chat sessions, chat services, billboards, newsgroups, and websites pertaining to child pornography or a sexual interest in children;

g. any computer-related documentation, which consists of electronically stored material that explains or illustrates how to configure or use computer hardware, software, or other related items;

h. any and all records and materials, in any format or media (including, but not limited to, e-mail, instant message chat logs, electronic messages, other digital data files, and web cache information), pertaining to the payment for or possession, receipt, shipment, or distribution of visual depictions of minors engaged in sexually explicit conduct or relating to or demonstrating a sexual interest in children;

i. any and all records and materials, in any format or media (including, but not

limited to, e-mail, instant message chat logs, electronic messages, other digital data files, and web cache information), identifying persons transmitting any visual depiction of minors engaged in sexually explicit conduct or demonstrating a sexual interest in children;

j. records of communication between individuals concerning the topic of child pornography, having sex with children, the existence of sites on the Internet that contain child pornography or that cater to people with an interest in child pornography, or membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to their members and constituents;

k. evidence of any online storage, e-mail, or other remote computer storage subscription, including, but not limited to, unique software relating to such subscription, storage, or email, user logs, archived data that shows connection to such service, or user login and password for such service;

l. any and all data, information, or images evidencing or revealing the unauthorized use of the device by a person other than an owner or authorized user, through the use of viruses, Trojan horses, or other malicious software or infiltration methods.

7. It is also requested for evidentiary purposes that this Court grant authorization for law enforcement personnel to videotape and photograph the interior of the subject location; to process the subject location for fingerprints; to analyze, test, and in any way scientifically process the subject location and all items seized; and to permit the entry and assistance of individuals who, by their experience and training, are qualified to assist in the execution of this warrant as designated by police or other law enforcement officials, for the purpose of examination, processing, and/or removal of any forensic evidence as described in Paragraphs 5 and 6 of this application and their subparagraphs.

8. With respect to the stored electronic data, information, and images contained in computers and other electronic devices described above and/or their components and accessories, it is also requested that this Court grant permission to retrieve the above-described data, information, and images, and print them or otherwise reproduce them by converting them or copying them into storage in another device.

9. This affidavit is based on my training, experience and personal observations, and information supplied to me from sources mentioned in the paragraphs below.

10. Based on my training and experience, including my interviews with suspects regarding collections of child pornography, I have become very familiar with the methods used by individuals to obtain, store, and trade in child pornography, including the following:

a. People who collect and trade in child pornography typically do not destroy or delete image or video files depicting child sexual abuse.

b. Collectors of child pornography typically retain their materials and related information for many years. These individuals retain their material indefinitely for the purpose of sexual gratification and sharing with others.

c. Individuals in possession of files containing sexual abuse are likely to save and maintain these files on their computer or other portable storage devices so it is accessible to them in their home or office.

d. Because of the illegality and the severe social stigma child pornography images carry, these individuals hide them in secure places, such as hidden files on the hard drive of the computer, external storage media or cloud storage.

e. I have experience and knowledge in the methods of communications that may be utilized through a computer, including but not limited to emails, chat rooms, instant messaging, peer to peer

networks, as well as basic skills in the recording and storage of online communications.

f. Files are maintained indefinitely on a computer.

g. Deleted files can usually be recovered during a forensic examination.

h. One of the goals of the investigation is to determine whether there are other persons within this jurisdiction possessing or distributing child pornography and ultimately identify any persons who are engaged in the direct exploitation of children by creating and publishing child pornography. Lists of email addressed, buddy lists and telephone numbers of persons they have contacted whether as potential victims or persons who share similar interests and materials are frequently maintained on their computers and storage media, as well as on their cell phones, electronic calendar/address books, and personal communication service devices.

11. With a computer connected to the internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of ways, including modem, local area network, wireless and numerous other methods.

12. Any computer accessing the Internet is assigned a unique Internet Protocol (IP) address. An IP address is a set of numbers which identify a specific computer on the internet. IP addresses follow the format of a series of sixteen numerals, which are organized in four groups of three numerals that are separated by a period, or: ###.###.###.###, wherein each of the number are between 0 and 255. Computers use IP addresses to identify each other on the internet. Thus, because a computer accessing "Outlook" (Microsoft) must be connected to the Internet, that device is identifiable by its IP address. Thus, investigators are able to determine the IP address of any computer using Microsoft services by issuing a subpoena to Microsoft. Then, investigators can search a public database compiled by the American Registry of Internet Numbers to determine the Internet Service Providers ("ISP") assigned to that specific IP address.

13. When a subscriber of an ISP wishes to access the internet via their service, the ISP will assign that account an IP address which identifies that account holder on the internet. By providing the ISP with the dates, times and IP addresses which a suspect used to access the internet, the ISP will be able to provide the identifying information for the account holder who was assigned that specific IP address at that date and time, if the records still exist on their system.

14. On or about November 28, 2017, I applied for and was granted by the Honorable John Hecht of this Court a search warrant [cited as KSC 1030-2017] to seize and search the records of four Facebook Accounts which are all tied via IP addresses to an individual known to me as Jonathan Deutsch ("Perpetrator"). NYPD received notification reports from The National Center for Missing and Exploited Children ("NCMEC") Cyber Tipline, and Facebook Inc., reporting images and videos of minor children in sexually explicit poses and performing sexual acts, which was the basis for the aforementioned warrant.

15. The warrant referred to above, KSC 1030-2017, is attached and I ask this Court to incorporate its contents by reference. Said warrant detailed the content of the communications between the perpetrator and the underage minors, including graphic language, and graphic and sexually suggestive photos and videos that the perpetrator coerced the children ("victims(s)") to provide. Said warrant also details the connection between the four Facebook accounts, i.e. that all the accounts were traced to the perpetrator through machine cookies, IP addresses, and email accounts captured along with said images. The following IP addresses were captured from these Facebook.com images and confirmed through the perpetrator's Google accounts via his email addresses; the **IP address 24.44.166.55, 69.112.4.72 and 47.18.138.69**. Specifically, these IP addresses were captured when the user of said Facebook.com accounts accessed these accounts and logged into these accounts via hardline during these sessions and during which, these images were uploaded by the victim and downloaded by the user ("perpetrator") of the Facebook.com account.

16. I am informed by Optimum, pursuant to a subpoena, that the **IP address 24.44.166.55, 69.112.4.72 and 47.18.138.69**, which is the IP address of the Optimum wireless service account

issued to listed subscriber Jonathan Deutsch, at 2785 W. 5th Street, Apt. 12C, Brooklyn NY 11224 (the perpetrator and the subject location).

17. I further state that the official records of the New York Department of Motor Vehicles indicate that the perpetrator provided his address of record as 2785 W 5th Street, Apartment 12C, Brooklyn, New York, which is the subject location.

18. I was in front of 2785 W 5th Street, Apartment 12C, Brooklyn, New York on December 18 , 2017, and I determined that there were no open wireless connections in the area of the location on that date and that I was also able to capture a list of wireless networks in the vicinity. I am aware that a forensic examiner can obtain the name of the wireless network utilized by a computer or device connecting to the internet.

19. I state that I was in front of 2785 W 5th Street, Apartment 12C, and made the following observations: 2785 W 5th Street is a twenty-one story brick building located between Mitchell Wesson Place and Neptune Avenue in Brooklyn, NY. The subject location is on the twelfth floor of this building. To access the subject location one enters the front entrance of the building which is clearly marked "2785" on the brick facade above the front door. The subject apartment is on the 12th floor and is clearly labeled "12C."

20. Based on the above facts, it is reasonable to conclude that a user of a computer and other electronic mediums, including but not limited to cellular telephones, located at the subject location is in possession of child pornography and distributed child pornography, and that evidence of the offenses of possessing and promoting a sexual performance by a child is currently located at the subject location.

21. Based on the above, I have reason to believe that the evidence related to the above-mentioned crimes may be found inside the subject location and within and upon computers, cellphones and any and all electronic devices, and other electronic devices capable of storing data, information, and images, and the electronic storage media recovered from the subject location.

22. Request is also made for a determination, pursuant to C.P.L. §690.40(2), that the executing officers be authorized to enter the premises to be searched without giving notice of authority or purpose, at any time of the day or night on the ground that there is reasonable cause to believe that the property sought may be easily and quickly destroyed or disposed of, by discarding them outside the premises through windows and other means of ingress and egress, corrupting the files, throwing the property in/under water, and that electronic records and other records can be easily deleted and/or erased, and further because the National Center for Missing and Exploited Children (NCMEC) has classified the case as a "Priority 1," i.e. that children are in danger.

WHEREFORE, I respectfully request that the court issue a Warrant and Order of seizure, in the form annexed, authorizing the search of the subject location, including all rooms, storage areas, any safes, cabinets, closets, strongboxes, desks, suitcases, briefcases or other such enclosures where property can be stored, for the above enumerated property, as well as the taking of videotape recordings and photographs of the above premises.

I also request that the Court authorize that with respect to any computers, cellular telephones, and other electronic storage devices, the warrant be deemed executed at the time said devices are seized and removed from the subject location, and that the search of said devices may continue thereafter for whatever reasonable time is necessary to complete a thorough search pursuant to this warrant. Once said computers and other devices are seized pursuant to the warrant, the data, information, and images contained therein will not change, and thus no greater intrusion will result from a thorough search being conducted within a reasonable.

I also request that the Court authorize a search and forensic examination of any computers, cell phones and any other electronic devices, and electronic storage media within and upon them, if found inside the subject location, for the internet browsing history, keyword searches, stored

documentation, file images, addresses, pages and any other electronic information, photo images (including video images), any information concerning computer passwords, encryption, web-sites, screen names or electronic mail addresses, any deleted files and all images, databases of personal identification information and contact list, and any data related to identity theft; any other data which would indicate ownership or use of the searched property and concerning the identification of individual(s) involved in said crimes;

I also request that the search and forensic examination of the evidence be performed at the subject location and/or in a controlled environment until such examination is complete;

I also request that a search of all files and data stored in computers, cellular telephones, and other electronic storage devices, irrespective of how the data is filed, labeled, designated, encrypted, hidden, disguised, or otherwise stored;

I also request that because of the sophisticated nature of the electronic devices that are subject of this warrant, this search be conducted in a manner consistent with reasonable technical and forensic evidence recovery practices employed in the recovery of the kinds of evidence described above, including but not limited to the use of any related software, peripheral devices used for data storage or battery charging. Because of the technical nature and volume of evidence sought and the nature of the location to be searched, authority is being requested to employ forensic electronic devices and software designed to facilitate searches of electronic devices of the kind described in this warrant and its supporting application and, if necessary to seek assistance from New York City Police Department personnel and/or from representatives of the manufactures of both the hardware and software during the execution of the device and for authority to conduct this search over a reasonable period beginning at the date and time the subject computer, is delivered to the location where the electronic forensic search is to be conducted. Additionally, it is requested that the search continue past the recovery of the first pertinent records and documents in any format, including electronically stored data and/or communications, information, images, text messages, e-mails, instant messages, contacts (names, addresses, telephone numbers, e-mail addresses), and continue until all such pertinent electronically stored evidence is recovered;

I also request that in the event that during the execution of the warrant with regards to the search of the computers and other electronic devices, and electronic storage media within and upon them, by the Kings County District Attorney's Office and/or New York City Police Department, it is necessary to utilize the assistance of others with expertise in decoding and/or obtaining password protections and/or encryptions, and in transferring, downloading, converting, dumping or draining from the memories of such electronic devices, such expert assistance may be sought and that such experts may be members of law enforcement organizations, industry trade associations, or from companies which manufacture or service such electronic devices or telecommunications industries; and

TOGETHER with such other and further relief that the Court may deem proper;

It is further requested that this affidavit remain sealed until otherwise directed by the court except for one copy at the Kings County District Attorney's Office, until needed for the prosecution resulting from the execution of this warrant.

No previous application has been made for a search of the subject location or property therein to any other Court, Judge, Justice, or Magistrate.

Sworn to before me this
December 22, 2017
Time: 12:30 pm

[redacted]

[redacted]
Detective Sheldon Spence,

LEAU SW No. 479/17
Prepared by: ADA Grace K. Hogan
December 22, 2017

HON. DANNY K. CHUN DEC 22 2017
JSC

[redacted]

Shield Number 4739,
NYPD Special Investigations Division

HON. DANNY CHUN
Justice, Supreme Court

HON. DANNY K. CHUN
J.S.C.

DEC 22 2017

COURT REPORTER

ATTACHMENT A

The property to be searched is: (1) One Gray Apple MacBook Pro Laptop, Serial number CPWJLK7KDTY3; (2) One Gray Apple MacBook Air Laptop, Serial number C02N900XG6D5; (3) One Gray Apple Ipad, Serial number DLXH7Z6MDJ8T; (4) One Black Apple Iphone X; (5) One Apple Iphone 6, Model number A1549, IMEI number 354411063842612; (6) One Apple Mac Mini, Model A1283, Serial number YM0081P39G5; (7) One Gray Apple iMac, Model number A1225, Serial number QP9300WQ0TM; (8) One black and gray Ultra External Hard Drive; (9) One Black Western Digital (WD) External Hard Drive, Serial Number WCAWZ0891570; (10) One Black Western Digital External Hard Drive, Serial number WCAVY2086429; (11) One Black Western Digital External Hard Drive, Serial number W0A8J1962444; (12) One Sabrent External Hard Drive, Serial number 60375028908214; (13) One Seagate External Hard Drive, Serial number NA8JECKX; (14) One Black Seagate 160 GB External Hard Drive, Serial number 5JS3S1E0; and (15) One Black Seagate 250 GB External Hard Drive, Serial number 5NF0T2HT, hereinafter the "Devices."

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A constituting evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A:

a. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt or distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2552 and 2552A, in any form wherever they may be stored or found;

b. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

c. Records, information, or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in Title 18, United States Code, Section 2256, including but not limited to:

i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to or transmission through interstate or foreign commerce, including by

United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined by Title 18, United States Code, Section 2256; and

ii. Records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or computer of any visual depiction of minors engaged in sexually explicit conduct, as defined by Title 18, United States Code, Section 2256;

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.